GSA e-PM and Internet Security Workshop

# Private Sector Security Technologies & Business Issues

James Lee

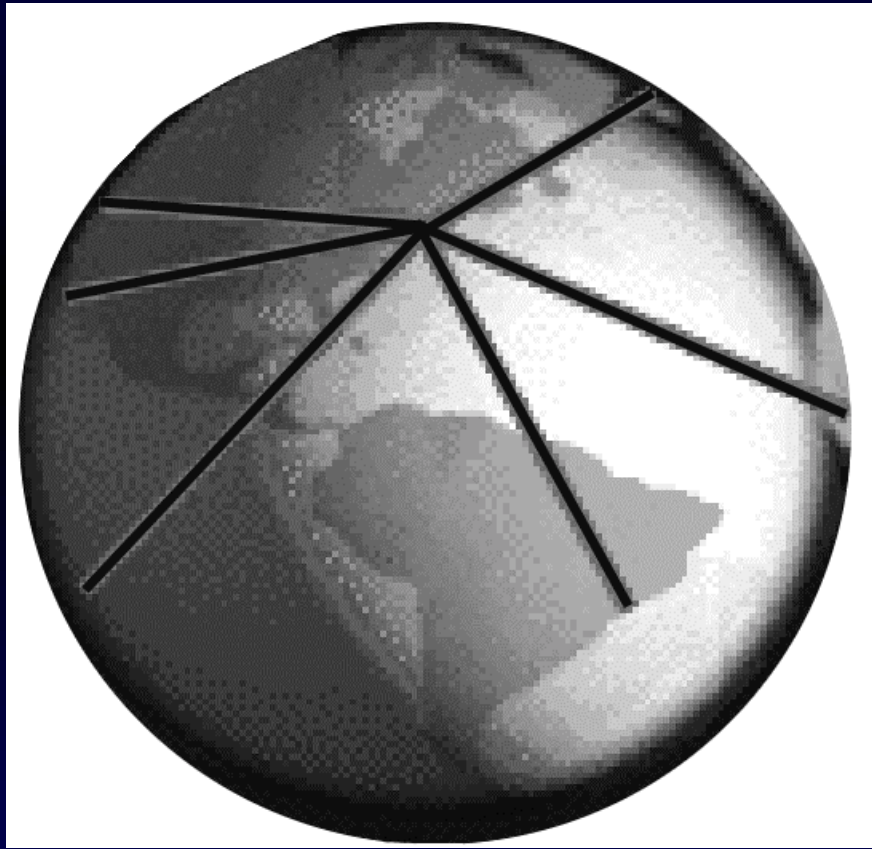
*Security Technologist*

*Oracle Service Industries*

ORACLE

# The Internet Changes Everything

- Low cost communications
  - More users = more security issues
- Standards based
  - HTML, HTTP, JAVA, CORBA, IIOP
- High availability worldwide
  - ANY Data, ANY browser, ANY time...



ORACLE

# Security Attacks on Fortune 1000

- 1999 Losses up 43%
  - some undetected, others not reported
- 40% were from Internet, 60% Intranet
- $800,000 losses per intrusion
  - How many intrusions can you afford?
  - Lost Confidence
- Most admitted at least one break-in
  - All that's needed is a basic packet capture product

Sources: 1999 Computer Security Institute and FBI Survey
*Information Security* 1999 Industry Survey

ORACLE

# Private Sector Issues

- Effective Internet Presence Critical to Survival (Physical vs. Virtual)
- Security #1 Priority & Impediment
- Use Existing Brand to Drive Customer Confidence
- Liability & Due Diligence Concerns
- Matching Security to User Group Requirements
- Industry Groups to Drive Standards

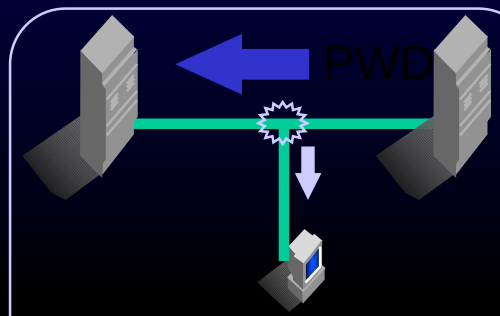
ORACLE

# Critical Infrastructure Protection Directive

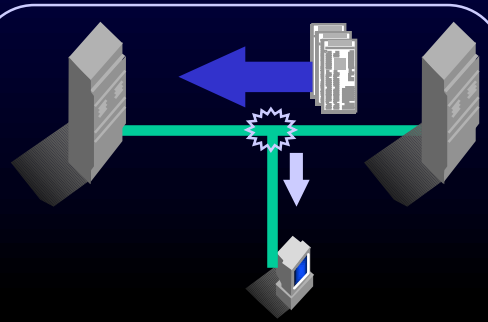

- Presidential Directive
- FBI & Private Industry
  - National Infrastructure Protection Center
  - InfraGard
- Protect U.S. Infrastructure
  - Banking & Finance
  - Communications
  - Utilities
  - Government Operations

ORACLE

# Common Security Breaches



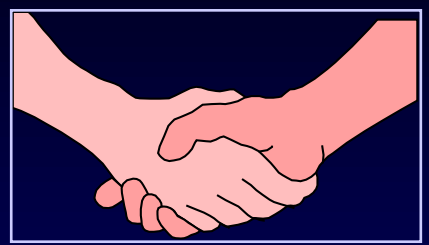

PASSWORD SNOOPING



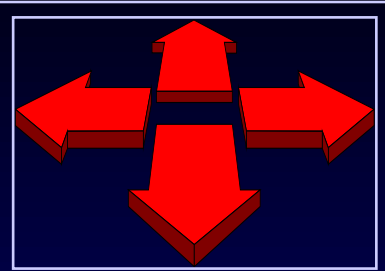
DATASTREAM SNOOPING


DATASTREAM MODIFICATION

ESTABLISHING USERS & AUTHORIZATIONS



USERS HAVE TOO MANY PASSWORDS



DISTRIBUTED SECURITY ADMINISTRATION

ORACLE

# Security - The Challenge

- Security without Compromise
  - Stronger Security for Competitive Advantage NOT Customer Deterrent!
  - Neutral or Beneficial to Bottom Line (ROI?)
  - Flexible (applies to multiple systems)
  - Minimal Impact on Existing Systems
  - Proven (so you don’t have to)

ORACLE

# Security Requirements

- Standards Compliant
- Evaluated Systems
- Architecture Flexibility
- Legacy Application Support
- Scalability and Performance
- Ease of Use
- Reduced Administration

ORACLE

# Security Requirements - Standards

- Why Security Standards?
  - Flexibility
  - Faster to Market
  - Vendor Interoperability
  - Industry Interoperability

ORACLE

# Security Requirements - Standards

- Critical Security Standards
  - **Common Criteria EAL3/4**
  - **LDAPv3**
  - **SSL**
  - **X.509v3**
  - **DoD PKI**
  - **PKCS 12, 7, etc.**
  - **FIPS 140-1**
  - **Kerberos**
  - **RADIUS**
  - **IPSec**

ORACLE

# Desired Security Features

- Identification & Authentication
  - **Passwords**
    - Password Management
  - **Single Sign-on**
    - Centralized (e.g., Kerberos)
    - Distributed (public key-based, X.509v3, SSL)
  - **Biometric**
  - **Card or Token (e.g., RADIUS, SecurID)**

ORACLE

# Desired Security Features (cont.)

- Access Control
  - **Discretionary**
    - Privileges, Roles, Views, Stored Procedures, Triggers
  - **Mandatory**
    - Multilevel Security
    - B1 Assurance
  - **Hybrid**
    - Virtual Private Databases
    - Virtually Separate but Physically Centralized

# Desired Security Features (cont.)

- Confidentiality and Integrity
  - Multiple encryption algorithms
  - Automatic key management and negotiation
- Security Management
  - Centralized Authorization (LDAPv3 Directory)
  - Certificate Authority
- Auditing
  - Configurable
  - Identity-based
  - Reduction Tools

ORACLE

# Example Systems

- Objectives
  - Example #1: Administrative Cost Reduction
  - Example #2: Ease of Use and Security
  - Example #3: Increased Accountability and Confidentiality
- Industries
  - Commercial
  - Government
  - Healthcare

ORACLE

# Example #1: Business Problem

- High Cost of Password Management
  - Large User Population (10,000+)
  - Multiple Systems/Multiple Passwords
  - Internal and External System Access
  - Accountability

ORACLE

# Solution - Card-based Authentication

- **Technologies**
  - Secure DBMS
  - RADIUS Card Authentication
- Benefits
  - Stronger Security (2 factor authentication)
  - Same mechanism for Multiple Systems
  - Reduced Cost of Issuing Passwords
  - Ease of Use
  - Accountability

ORACLE

# Example #2: Business Problem

- Need for Stronger Security
  - Large Airport
  - Cargo Tracking and Security
  - Verification of Delivery
  - Accountability

# Solution - Strong Authentication

- **Technologies**
  - Secure DBMS
  - Biometric Authentication
  - Audit
- Benefits
  - Stronger Security
  - No End-User (Trucker) Training
  - High Accountability
  - Reduced Paperwork

ORACLE

# Example #3: Business Problem

- Accountability and Confidentiality
  - Largest non-profit health plan in U.S.
    - 8.6 million members
    - $14.6 Billion annual revenues
  - Patient Record Security
  - Paper-based Systems
    - Accountability of Access
- Quality Care at a Lower Cost

ORACLE

# Operational Challenge

- 300 points of care
- 55,000+ simultaneous users
- 1000’s of patients per day
- 20-50 billion messages per day
- 2-4 terabytes of data per year

ORACLE

# Electronic Medical Records System

- Secure on-line access to patient records and medical research
- Collaboration between doctors, nurses, technicians
- Point-of-care
  - in examination rooms
  - on phone lines at call centers
  - over Internet

ORACLE

# Solution - Strong System Security

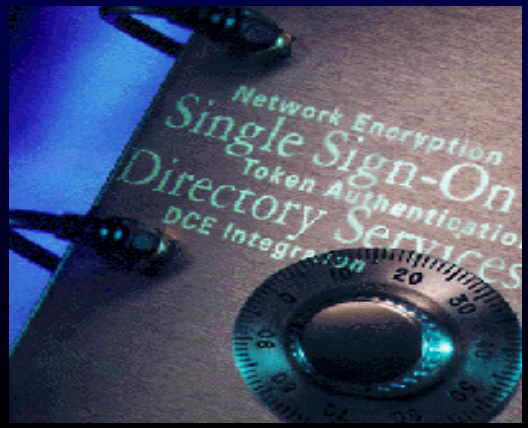
- **Technologies**
  - Secure DBMS
  - Authentication
  - Encryption
  - Workflow Rules for Procedures and Treatment
  - Audit
- Benefits
  - Higher Accountability over Paper-based Systems
  - Encryption Satisfies Patient Privacy Issues
  - Faster Information Access = Better Healthcare

ORACLE

# Summary - Security Requirements

- Standards Compliant
- Evaluated Systems
- Architecture Flexibility
- Legacy Application Support
- Scalability and Performance
- Ease of Use
- Reduced Administration

ORACLE




# Oracle Security Products:

*Security Without Compromise™*